Spear phishing : Menaces et tendances principales

Vol. 5 Décembre 2020

Bonnes pratiques pour se protéger contre des attaques en constante évolution

Comme le montre la vitesse avec laquelle ils ont exploité les peurs liées à la pandémie de COVID-19, les cybercriminels s'adaptent rapidement à l'actualité et aux nouvelles techniques. Ce rapport détaillé propose un examen de l'évolution des tendances en matière de spear phishing, ainsi que les nouvelles méthodes adoptées par les pirates pour piéger leurs victimes.»

Barracuda
Your journey, secured.

Table des matières

Résultats clés 1

Vue d'ensemble des attaques de spear phishing 2–4

Tendances des attaques de spear phishing 5

Les hackers « travaillent » en même temps que leurs cibles 6

Attaques de spear phishing liées à la COVID-19 7

Attaques de phishing latéral 8

URL malveillantes contenues dans les e-mails de spear phishing 9–10

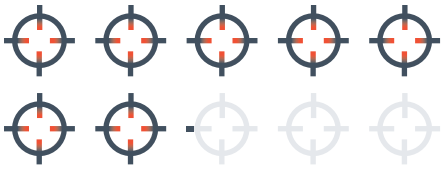
Redirections d'URL dans les attaques de spear phishing 11

Bonnes pratiques de protection contre le spear phishing 12

Résultats clés

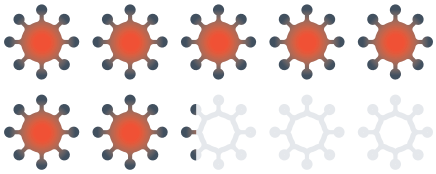
12 % des attaques de spear phishing sont de type BEC

Les attaques de type Business email compromise (BEC) représentent 12 % des attaques de spear phishing analysées, en augmentation par rapport aux 7 % constatés en 2019.



71 % des attaques de spear phishing contiennent des URL malveillantes

Les pirates exploitent diverses techniques pour maquiller les liens malveillants et contourner toute détection par les solutions de protection des URL.

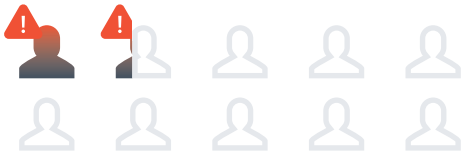


72 % des attaques liées à la COVID-19 sont des escroqueries

À titre de comparaison, les escroqueries représentent 36 % des attaques, tous sujets confondus. Les pirates se servent de la COVID-19 dans leurs escroqueries peu ciblées, axées sur de faux remèdes et des fausses campagnes de dons.

Seuls 30 % des attaques de type BEC contenaient un lien

Les hackers utilisant la technique du BEC cherchent à gagner la confiance de leur victime et attendent une réponse à leurs e-mails, l'absence d'URL rendant la détection de l'attaque plus difficile.



13 % des attaques de spear phishing proviennent de comptes internes compromis

Les entreprises doivent investir dans une solution qui protègera le trafic de leur messagerie interne, et ce, au même titre qu'elles se protègent contre les expéditeurs externes.

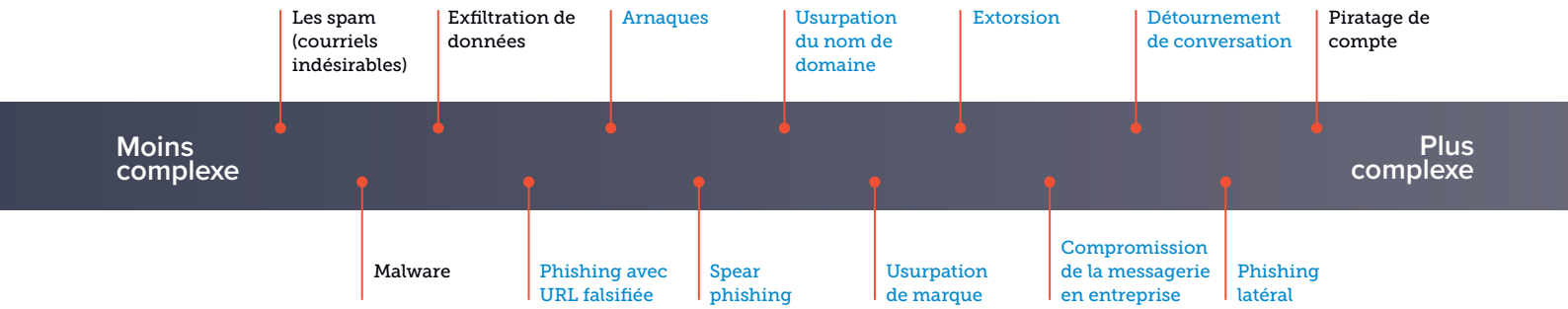
Vue d'ensemble des attaques de spear phishing

Les chercheurs de Barracuda ont identifié 13 types de menaces par e-mail auxquelles les entreprises sont confrontées aujourd'hui. Il peut s'agir aussi bien d'attaques à grande échelle telles que les spams ou les malwares, que de menaces plus ciblées utilisant l'ingénierie sociale, comme par exemple l'usurpation d'identité et la compromission de la messagerie en entreprise.

Certaines de ces attaques sont menées conjointement à d'autres. Les pirates utilisent en effet souvent plusieurs techniques simultanément. Par exemple, de nombreuses attaques d'usurpation d'identité de marques incluent des URL de phishing, et il n'est pas rare que le détournement de conversations fasse partie de la compromission de la messagerie en entreprise. Comprendre la nature et les caractéristiques de ces attaques vous aidera à concevoir une meilleure protection de vos activités, vos données et vos équipes.

Cette étude se concentrera sur neuf des attaques les plus complexes et les plus ciblées, notamment :

13 types de menaces par e-mail : Types de menaces par e-mail analysés dans cette étude.



Les hackers privilégiaient habituellement les attaques via des malwares, mais ces dernières années ils se sont tournés vers les ransomwares et les attaques de phishing ciblées, dans le but de récupérer les identifiants des utilisateurs.

Les attaques de spear phishing augmentent en volume, en complexité et ont un impact de plus en plus important sur les entreprises. Elles sont minutieusement étudiées et ciblées et affichent un taux de réussite beaucoup plus élevé lorsqu'il s'agit de contourner les mécanismes de sécurité des e-mails, d'atterrir dans la boîte de réception des utilisateurs et des les inciter à passer à l'action. Cette recherche se concentre sur les tendances associées à ces attaques d'ingénierie sociale, les nouvelles tactiques des cybercriminels, l'évolution des menaces dans le temps et les mesures que les entreprises peuvent prendre pour s'en prémunir et les contrer.

Les chercheurs de Barracuda ont recensé plus de 2,3 millions d'attaques de spear phishing entre août et octobre 2020, impliquant plus de 80 000 entreprises aux quatre coins du monde.

Toutes ces attaques par e-mail ont été classées en cinq catégories principales :

Phishing (hameçonnage)

Cette catégorie d'attaques utilise diverses tactiques d'usurpation d'identité dans le but de faire croire aux personnes qu'elles reçoivent un e-mail de la part d'une marque ou d'un service qu'elles ont déjà utilisé, notamment :

- **L'usurpation de marque** : des attaques qui usurpent l'identité de marques ou d'entreprises bien connues
- **Les attaques par formulaire** : les pirates exploitent les sites de téléchargement de fichiers, partage de contenu et de productivité tels que sway.office.com
- **Les attaques de phishing avec pièces jointes**
- **Le phishing d'URL** : les cybercriminels envoient un e-mail à leurs victimes les invitant à saisir des informations confidentielles sur un site Web frauduleux présenté comme un site légitime
- **Le spear phishing** : une attaque de phishing par e-mail hautement personnalisée, généralement conçue pour voler des informations confidentielles, telles que des identifiants de connexion ou des données financières

Compromission de la messagerie en entreprise (BEC)

La compromission de la messagerie en entreprise (BEC), également connue sous le nom de whaling, arnaque au président ou fraude au virement, est une menace qui prend rapidement de l'ampleur. Les hackers usurpent l'identité d'un employé, fournisseur ou toute autre personne de confiance dans leur intérêt financier. Voici quelques tactiques que les chercheurs de Barracuda ont pu constaté récemment :

- **Fraude au virement** : demandes de transfert d'argent frauduleux vers un compte illégal.
- **Arnaque à la paie** : demandes frauduleuses de modification des coordonnées bancaires pour le paiement des salaires.
- **Arnaque aux cartes-cadeaux** : demandes frauduleuses d'achat et d'envoi de cartes-cadeaux.
- **Détournement de conversations** : également connu sous le nom d'escroquerie à l'usurpation d'identité des fournisseurs. Les cybercriminels détournent ou s'immiscent dans des conversations entre un fournisseur et une entreprise, demandent un paiement ou apportent une modification de dernière minute aux détails du paiement, détournant ainsi l'argent vers des comptes illégitimes.
- **Usurpation de nom de domainen** : les pirates tentent de se faire passer pour un domaine, à l'aide de techniques telles que le typosquattage.

Extorsion

Dans ce type d'attaque, le hacker entre en contacte par e-mail avec des victimes potentielles et prétend détenir des vidéos ou des informations compromettantes qui seront diffusées au public si la victime ne paie pas. Pour « prouver » qu'il détient bien ces informations, l'e-mail contient des données sensibles que seule la victime est censée connaître, comme ses mots de passe par exemple. Selon le FBI, le coût des attaques d'extorsion dépassait les 107 millions de dollars en 2019.

Phishing latéral

Les attaques de phishing latéral proviennent généralement de comptes compromis et prennent pour cibles les utilisateurs internes à des entreprises. Ces attaques sont difficilement détectables car elles proviennent de comptes de messagerie internes légitimes et semblent provenir d'un collègue de confiance. Dans ce rapport, ce type d'attaques internes est examiné séparément des attaques externes (escroquerie, extorsion, phishing et BEC).

Arnaques

L'escroquerie par e-mail est un type d'attaque de spear phishing dont le but final est d'usurper l'identité de la victime ou encore de l'inciter à divulguer des informations personnelles. Dans de nombreux cas, de fausses factures ou associations caritatives et bien d'autres stratagèmes sont utilisés afin de soutirer de l'argent à la victime. Voici quelques exemples d'escroqueries que les chercheurs de Barracuda voient régulièrement :

- **Arnaque au faux support techniques** : une entreprise malhonnête vous informe de la présence d'un virus sur votre appareil et vous invite à faire appel à ses services (payants) pour remédier au problème.
- **Arnaque au transfert d'argent venu de l'étranger** : une personne vous propose une importante somme d'argent si vous l'aidez à transférer des fonds hors de son pays, mais vous devez d'abord avancer de nombreux frais (honoraires, taxes).
- **Arnaque au don caritatif** : suite à une tragédie nationale ou personnelle, des escrocs vous contactent par e-mail afin de vous inviter à faire un don au profit des victimes. Bien entendu, l'argent récolté n'est pas reversé aux victimes ni à une quelconque association légitime, mais profite aux pirates.
- **Arnaque au don à des partis politiques** : pendant les élections, les escrocs envoient des e-mails demandant des dons pour soutenir un candidat ou une organisation politique, mais ces dons profitent au criminel.

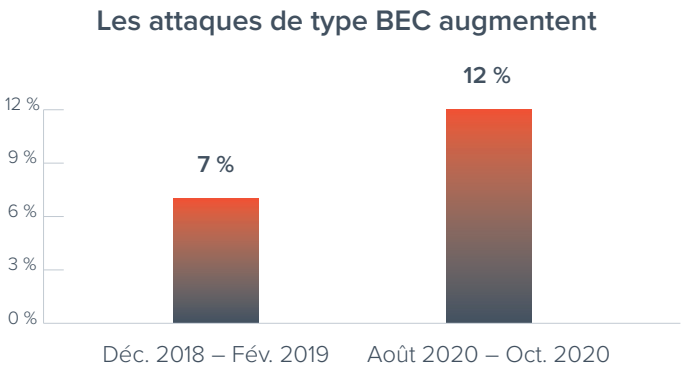
Selon le rapport Internet Crime Report de 2019 établi par le FBI, le montant des pertes attribuées aux escroqueries par e-mail s'élève à 791 millions de dollars.

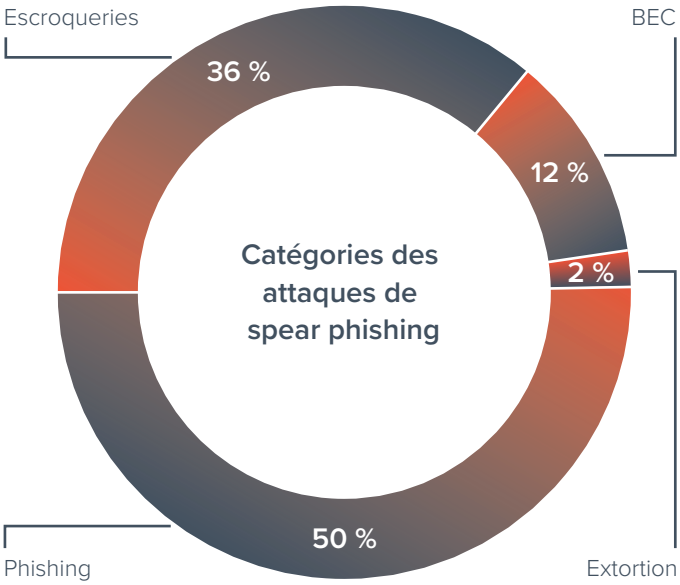
Tendances des attaques de spear phishing

Les attaques de phishing représentent la moitié (50 %) de toutes les attaques de spear phishing analysées par les chercheurs de Barracuda ces trois derniers mois, de loin la catégorie la plus importante. Ces attaques ciblent des individus avec l'intention de voler des informations confidentielles, telles que les identifiants de connexion.

La compromission de la messagerie en entreprise (BEC) est une menace de plus en plus importante. En mars 2019, des chercheurs de Barracuda ont rapporté que 7 % de toutes les attaques de spear phishing pouvaient être considérées comme BEC, mais aujourd'hui ce chiffre est passé à 12 %. Cette croissance rapide témoigne de l'efficacité de ce type d'attaque. Selon le FBI, les attaques de type BEC ont généré des pertes de plus de 3,5 milliards de dollars en 2019. Au cours des deux dernières années, une série d'attaques de type BEC furent très médiatisées, parmi elles, l'attaque de la société japonaise Toyota Boshoku Corporation (fournisseur de pièces automobiles) qui a perdu 37 millions de dollars en 2019, ou encore le gouvernement de Porto Rico, qui a perdu 2,6 millions de dollars début 2020.

Selon le FBI, ces attaques ont coûté plus de 26 millions de dollars aux entreprises entre 2016 et 2019.



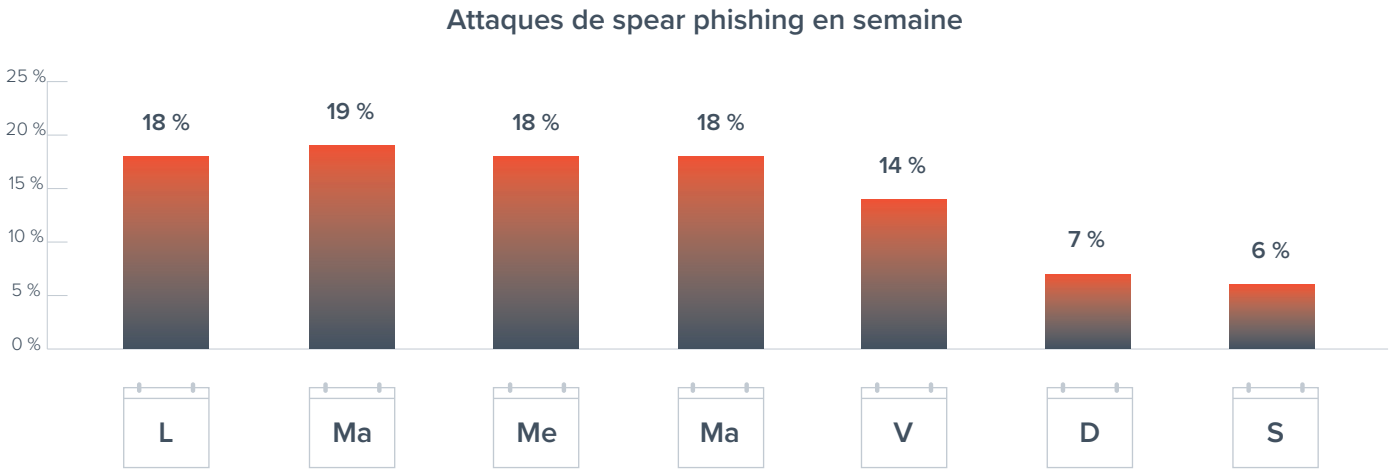


L'escroquerie et l'extorsion constituent le reste des des attaques analysées dans cette étude, représentant respectivement 36 % et 2 %. Ces attaques sont moins ciblées par nature, mais constituent pour autant une part importante de l'ensemble des escroqueries observées par les chercheurs de Barracuda. Aujourd'hui, les attaques par extorsion représentent une plus petite partie des attaques de spear phishing constatées par les chercheurs en 2019, soit 2 % contre 11 % en 2019. Ce phénomène ne résulte pas de la diminution du nombre des attaques par extorsion, mais plutôt de la croissance fulgurante des autres types d'attaques de spear phishing.

Les pirates informatiques « travaillent » en même temps que leurs cibles

Selon cette analyse, 87 % des attaques de spear phishing sont perpétrées pendant les jours ouvrés, lorsque la plupart des entreprises sont actives. Mais pour autant, il n'est pas rare que les hackers opèrent pendant les week-ends. Une demande urgente est envoyée par un cadre à un employé distrait, dans le but d'obtenir une réponse rapide :

> « Bonjour, J'espère que vous profitez bien de votre week-end. J'ai besoin de votre aide, merci de bien vouloir me répondre lorsque vous aurez reçu ce message. Merci »



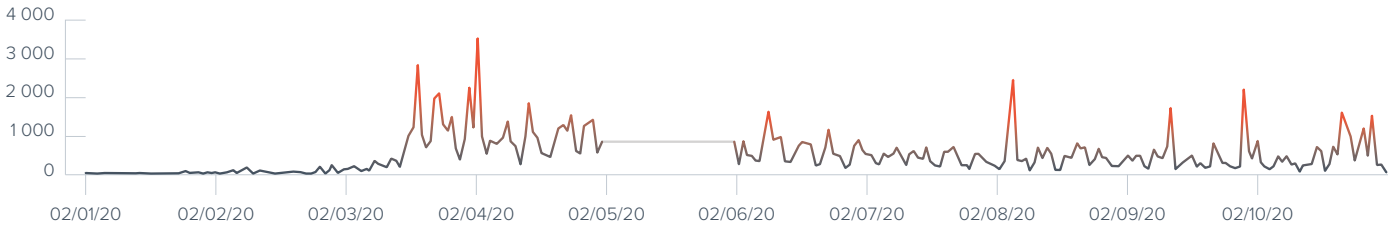
Les chercheurs de Barracuda ont constaté des baisses similaires pendant les fêtes, le 4 juillet par exemple, où le nombre d'attaques de spear phishing était 62 % inférieur à la moyenne. En revanche, les cybercriminels opèrent parfois pendant les vacances ou pendant certains événements saisonniers pour exploiter les failles et autres vulnérabilités de sécurité. La précédente étude de Barracuda sur les attaques de spear phishing dans le secteur de l'éducation a révélé que le nombre d'attaques prenant pour cibles les établissements scolaires et les universités augmentaient significativement en septembre, lorsque les élèves retournaient sur les bancs de l'école.

Attaques de spear phishing liées à la COVID-19

Plus tôt cette année, alors que le monde devait faire face à la nouvelle réalité de la pandémie de COVID-19, les chercheurs de Barracuda avaient constaté une augmentation constante du nombre d'attaques de spear phishing liées au coronavirus dès le mois de janvier, avec un pic significatif de 667 % début mars 2020.

Les chercheurs de Barracuda ont continué à suivre cette tendance sur 2020. Les hackers ne cessent d'utiliser la COVID-19 comme un appât dans leurs attaques, mais pour autant, le volume global de ces attaques n'a pas augmenté de manière importante depuis le mois de mars. Les attaques de spear phishing liées à la COVID-19 représentaient environ 2 % de celles détectées par Barracuda. Bien que l'intérêt des hackers pour ce type de spear phishing a quelque peu faibli, il n'a pas complètement disparu pour autant.

Attaques de spear phishing liées à la COVID-19 en 2020

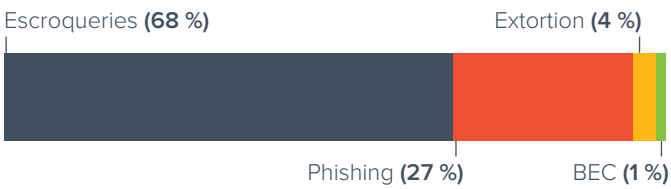


Les données pour la période du 1er mai au 1er juin n'apparaissent pas suite à un changement intervenu dans le processus de reporting interne.

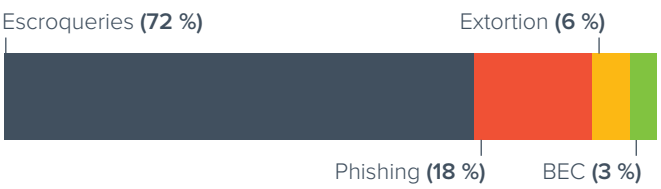
La grande majorité de ces attaques sont des escroqueries, principalement des messages appelant aux dons, à des investissements ou concernant des successions. Nous avons noté une légère augmentation du nombre d'attaques de type BEC utilisant la COVID-19 pour attirer l'attention de leurs victimes (de 1 % à 3 %), mais ces chiffres restent faibles par rapport à la moyenne globale de ce type d'attaques, soit 12 %.

Au début de la pandémie, les hackers ont su tirer profit de l'incertitude entourant la situation. En effet, alors que tout le monde apprenait à vivre avec cette nouvelle réalité, les cybercriminels se sont, quant à eux, intéressés à d'autres domaines, ce qui montre à quel point ils savent s'adapter rapidement.

Attaques de spear phishing liées à la COVID-19 janv. – avril 2020



Attaques de spear phishing liées à la COVID-19 juin – oct. 2020



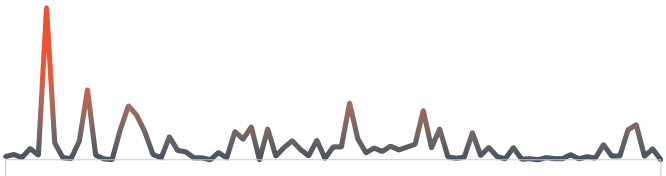
Attaques de phishing latéral

Jusqu'à présent, ce rapport concernait essentiellement les e-mails envoyés aux utilisateurs à partir de sources externes. Cependant, les chercheurs de Barracuda ont également constaté un certain nombre d'attaques de phishing latéral, c'est-à-dire des attaques de spear phishing perpétrées en interne, généralement à partir de comptes potentiellement compromis.

Les hackers corrompent un compte de messagerie professionnelle et l'utilisent pour lancer des attaques. Ces comptes sont très précieux à leurs yeux car ils constituent un tremplin idéal pour perpétrer d'autres attaques par e-mail au regard de la confiance importante associée aux e-mails envoyés à partir de ces comptes.

Dans cette analyse, les chercheurs de Barracuda ont pu constater que les pirates perpétraient des attaques de phishing latéral à grande échelle, leur but étant d'envoyer autant d'e-mails que possible avant que leur activité malveillante ne soit détectée et bloquée. Les pics observés dans le graphique des tendances indiquent qu'un nombre important de messages malveillants (souvent des milliers) sont envoyés à partir de ces comptes compromis.

Tendances des attaques de phishing latéral



1er août 2020 — 31 octobre 2020

Si l'on considère le nombre total de messages malveillants (provenant de sources internes et externes), environ 13 % d'entre eux peuvent être qualifiés de phishing latéral envoyés à partir de comptes de messagerie internes potentiellement compromis. Certains secteurs sont plus touchés que d'autres par le piratage de compte et la fraude par communication sortante. En début d'année, les chercheurs de Barracuda se sont penchés sur le secteur de l'éducation, fortement touché par ce problème. En effet, dans cette analyse, ils ont remarqué que les attaques par e-mails provenant de comptes compromis des établissements scolaires étaient plus nombreuses que les attaques externes.

E-mails de spear phishing : expéditeur interne contre expéditeur externe

Tous ces messages sortants ne visaient pas forcément la même entreprise que celle dont le compte a été compromis. En effet, la grande majorité de ces messages (85 %) visaient des interlocuteurs ayant un domaine de messagerie différent. Les entreprises peuvent utiliser différents domaines de messagerie en fonction des employés, toutefois on peut raisonnablement supposer que la plupart de ces messages visaient des utilisateurs externes.

Ces messages internes ne passent pas par les passerelles de messagerie, ce qui rend les entreprises vulnérables face aux menaces. Les messages envoyés depuis ces comptes compromis, en particulier ceux provenant d'un collègue, peuvent potentiellement afficher un taux de réussite plus élevé étant donné la confiance accordée aux messages envoyés par une personne de son entourage.

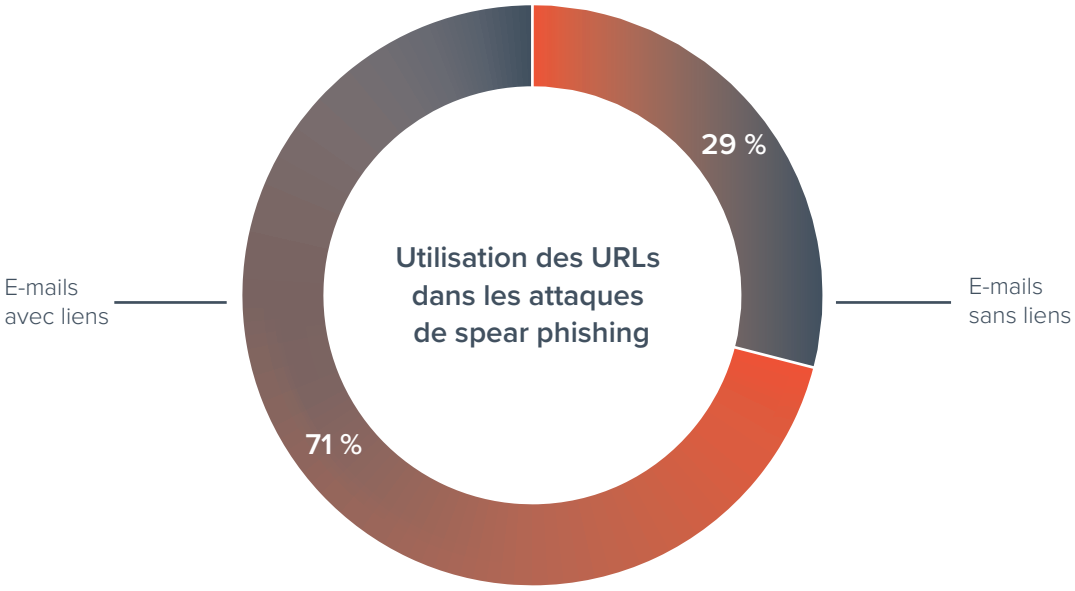
Les entreprises doivent investir dans la protection contre le piratage de compte, et ce, en analysant les messages envoyés en interne et en formant les utilisateurs à identifier un compte piraté et les e-mails provenant d'un compte compromis.

URLs malveillantes contenues dans les e-mails de spear phishing

La plupart des e-mails de phishing contiennent une URL, et les attaques de phishing plus ciblées ne font pas exception. Les pirates utilisent des tactiques d'ingénierie sociale soigneusement conçues pour inciter les utilisateurs à cliquer sur les URLs malveillantes incluses dans les e-mails. Environ 71 % des attaques de spear phishing examinées par les chercheurs de Barracuda dans cette analyse contenaient au moins une URL dans le corps de l'e-mail. Ces URL mènent généralement à un site de phishing utilisé par les pirates pour voler des identifiants de connexion ou distribuer des malwares.

Bien que de nombreuses entreprises disposent aujourd'hui d'une certaine forme de protection des liens, un nombre important de ces URLs contourneront les filtres de passerelle traditionnels.

Les cybercriminels exploitent des sites Web piratés ou des sites fraîchement enregistrés pour créer une réplique presque parfaite d'une page de connexion officielle. Ces messages contournent les dispositifs de détection pour atterrir dans les boîtes de réception des utilisateurs.

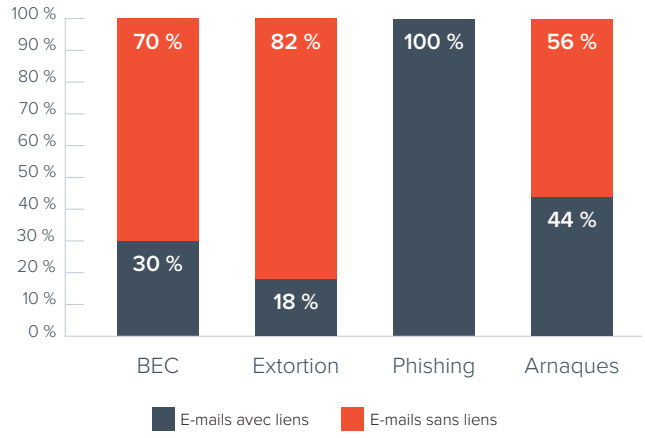


Les pirates incluent presque toujours un lien dans les attaques de phishing par e-mails car ils représentent un bon moyen de récupérer des données sensibles. Cependant, l'utilisation des liens varie selon le type d'attaque. Seuls 30 % des attaques de type BEC contenaient un lien. En général, l'objectif de ces attaques d'usurpation d'identité des employés est de gagner la confiance de la victime et d'obtenir un retour de sa part.

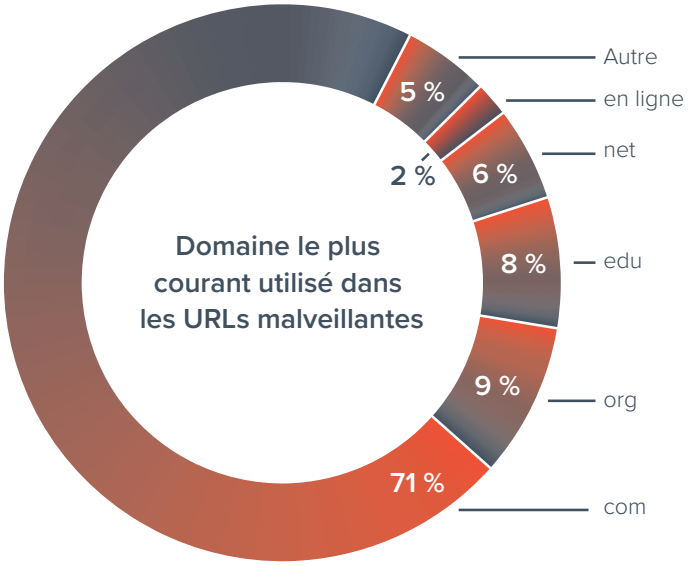
Dans les attaques d'extorsion en revanche, aucune réponse n'est attendue et les hackers ne cherchent pas à obtenir des identifiants de connexion.

Les pirates prétendent détenir des informations compromettantes supposément enregistrées sur l'ordinateur de la victime et menacent de divulguer ce contenu à tous ses contacts sauf si elle accepte de payer la somme réclamée. Le bitcoin est le mode de paiement généralement exigé, et les détails du portefeuille sont inclus dans le message.

Utilisation d'URLs pour les différents types d'attaques



Les domaines utilisés dans les URLs malveillantes ressemblent à ceux utilisés au quotidien. Le plus souvent, on retrouvera .com, que les gens ont pour habitude de voir dans leurs e-mails. Les cybercriminels adaptent également leurs attaques à leurs victimes en utilisant des techniques qui font paraître ces URLs plus légitimes. Par exemple, des domaines comme .edu sont couramment utilisés dans le secteur de l'éducation et permettent aux pirates de se faire passer pour un site ou un service familier.



Redirection des URLs dans les attaques de spear phishing

Les cybercriminels utilisent la redirection d'URL dans leurs attaques pour légitimer leurs e-mails de phishing. Ces URLs malveillantes redirigent le trafic vers un site malveillant. Ces liens peuvent sembler légitimes mais redirigent les utilisateurs finaux vers un site de phishing par le biais de plusieurs redirections.. Les pirates utilisent les redirections ouvertes de Google et d'Adobe car elles sont souvent incluses dans les listes des URLs autorisées de nombreuses solutions de sécurité.

Près de 4 % de tous les messages comportant des liens ont utilisé des redirections d'URL. Bien que les redirections d'URL représentent un travail supplémentaire pour les pirates, elles sont utilisées pour contourner la détection de liens de phishing connus.

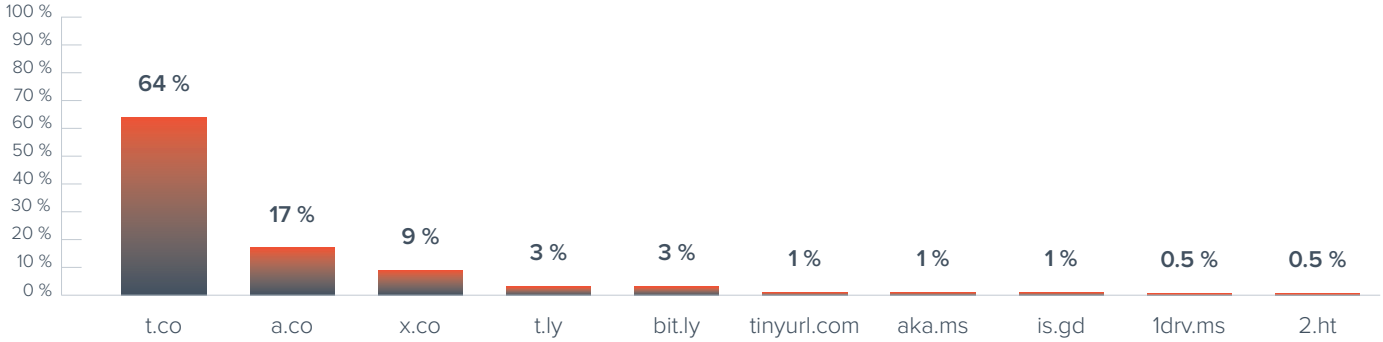
Utilisation d'un raccourcisseur d'URL dans les attaques de spear phishing

Les cybercriminels ont de plus en plus recours à des services populaires de raccourcissement d'URL tels que t.co, bit.ly, tinyurl.com et autres afin d'intégrer des liens malveillants dans leurs e-mails de phishing. Les raccourcisseurs d'URL réduisent la longueur du lien de sorte qu'il soit masqué par des lettres ou des chiffres aléatoires. Cette tactique dissimule la véritable destination du lien et permet aux pirates de tromper plus facilement leurs victimes.

Redirections d'URL dans les attaques de spear phishing

Comme tout autre message de phishing, les e-mails contenant des liens raccourcis semblent provenir d'entités connues avec des liens redirigeant les victimes vers des sites d'apparence légitime nécessitant des identifiants de connexion pour accéder aux informations. Les hackers ont recours à plusieurs services différents, avec une préférence pour t.co (le service Twitter pour raccourcir les liens) utilisé dans environ 64 % des attaques contenant une URL raccourcie.

Top 10 des services de raccourcissement d'URL utilisés dans les attaques de spear phishing



Bonnes pratiques de protection contre le spear phishing

Aujourd'hui, les entreprises sont de plus en plus exposées aux attaques de phishing ciblées. Pour protéger votre entreprise et vos utilisateurs, vous devez investir dans une technologie permettant de contrer les attaques et former votre personnel en conséquence pour qu'il constitue la dernière ligne de défense.

Technologie

- Tirez profit de l'intelligence artificielle. Les escrocs adaptent leurs e-mails pour contourner les passerelles et les filtres anti spam. Il est donc crucial de disposer d'une solution de détection et de protection contre les attaques de spear phishing, notamment la compromission de la messagerie en entreprise, l'usurpation d'identité et les attaques d'extorsion. Déployez une technologie dédiée ne reposant pas uniquement sur la détection de liens ou de pièces jointes malveillantes et utilisez le machine learning pour analyser les schémas de communication classiques au sein de votre entreprise pour repérer toute anomalie indiquant potentiellement une attaque.
- Déployez une solution de protection contre le piratage de compte. De nombreuses attaques de spear phishing latéral proviennent de comptes compromis ; assurez-vous qu'aucun pirate informatique n'utilise votre entreprise comme camp de base pour perpétrer ses attaques. Déployez une technologie qui utilise l'intelligence artificielle pour identifier les comptes compromis et corriger les problèmes en temps réel, en alertant les utilisateurs et en supprimant les e-mails malveillants envoyés par ces comptes.
- Mettez en œuvre l'authentification et le reporting DMARC. L'usurpation de domaines est l'une des techniques les plus couramment utilisées dans le cas d'attaques par usurpation d'identité. L'authentification DMARC et sa mise en œuvre peuvent empêcher l'usurpation de domaines et de marques, tandis que les rapports et les analyses DMARC permettent aux entreprises de les mettre en œuvre correctement.

Collaborateurs

- Formez votre personnel à reconnaître et signaler les attaques. Sensibilisez vos utilisateurs aux attaques de spear phishing dans le cadre des formations à la sécurité. Assurez-vous qu'ils savent les reconnaître, comprendre leur nature frauduleuse et les signaler. Faites des simulations de phishing par e-mails, messages vocaux et SMS afin qu'ils sachent identifier les cyberattaques, testez l'efficacité de votre formation et évaluez les utilisateurs les plus vulnérables aux attaques.
- Révisez les politiques internes. Aidez vos employés à ne pas commettre d'erreurs coûteuses en élaborant des procédures pour confirmer toute demande reçue par e-mail, y compris les demandes de virements bancaires ou l'achat de cartes cadeaux.
- Mettez en place une prévention optimale contre la perte de données. Utilisez la combinaison de technologies et de stratégies professionnelles adaptée pour garantir la confidentialité des e-mails contenant des informations confidentielles, personnelles ou sensibles devant être protégées et ne jamais sortir de l'entreprise.

Barracuda en quelques mots

Notre objectif : faire du monde un endroit plus sûr.

Chez Barracuda, nous pensons que chaque entreprise mérite un accès à des solutions de sécurité cloud de niveau professionnel, à la fois abordables, intuitives et facilement déployables. Nous protégeons vos e-mails, réseaux, données et applications à l'aide de solutions innovantes capables de s'adapter au parcours de nos clients et de se développer en conséquence.

Plus de 200 000 entreprises aux quatre coins du monde font confiance à Barracuda pour les protéger, même lorsque le danger ne leur semble pas imminent : nous nous voulons invisibles afin de permettre aux entreprises de se concentrer sur leurs activités et leur développement.

Pour en savoir plus, rendez-vous sur fr.barracuda.com.

Barracuda
Your journey, secured.